

March 17, 2006

Hon. Kenneth M. Karas
Judge, U.S. District Court
United States Courthouse
500 Pearl Street – Rm. 2260
New York, N.Y. 10007-1312
Fax No: 212 805-7968

Re: *United States v. Alberto Vilar* - 05 Cr. 0621

Dear Judge Karas:

I am writing on behalf of defendant Alberto Vilar to address the government's suggestion that the defendants re-review the materials designated as privileged. For the reasons set forth by Mr. Tanaka's counsel, this suggestion should be summarily rejected. In addition, I wish to reiterate the arguments we submitted to the Court by letter dated December 13, 2005 regarding the scope of the government's search of the Amerindo computers. For the reasons set forth therein and reiterated below, the Court should order the government to conduct key word searches of the computer systems to identify data for which they have established probable cause to search. That material should be segregated and the rest returned to the defendants. The defendants should only be put to the task of asserting privilege with respect to materials properly obtained pursuant to a particularized search.

As set forth in my December 13, 2005 letter, the seizure of the computers from the Amerindo offices presents a Fourth Amendment problem that requires a computer-age protocol. The government would no doubt agree that not all of the information and data on the Amerindo computer server and in the laptops would be subject to search and seizure under the warrant if the information and data existed in paper form. The fact that information exists on a computer should not exempt it from the particularity requirement of the Fourth Amendment. While we understand that in order to seize information in a computer, the government must seize the hardware, if the government has unrestricted access to information on seized computers, the Fourth Amendment becomes meaningless. We live in an age where documents are routinely scanned into and stored in computers and on disks. Just as searches of physical premises are circumscribed by the probable cause showing giving rise to them, searches of computerized information must be similarly circumscribed.

Page 2
March 17, 2006

In a traditional search of business premises, government agents look at documents, files and papers only long enough to make a determination whether the document, file or paper falls into one of the categories for which probable cause to search and seize has been established. If it fits into any of the specified categories, it is seized; if not, it should be left. The same procedure should be utilized with computer information, especially because it is easier and faster to search computer data than physical material, using particularized search terms or filters.

While the defendants' privacy rights in the Amerindo offices have already been violated - to the extent the court finds they were violated - the government's continuous searches through the computer data constitute ongoing violations that the Court has the power to stop. We suggest that the court, with the assistance of counsel, establish a group of permissible, particularized search terms that correspond to the probable cause showing. Those searches should be run and the information returned should be segregated, reviewed for privilege and made available to the prosecution team to the extent it is not privileged. The remaining information should be returned to Amerindo and the defendants.

If the government maintains its claimed right to access every corner and crevice of the entire body of computer information that existed at Amerindo, the defendants will be put to [and has already been put to] the extraordinary expense of doing a privilege review on hundreds of thousands of pages of computer information, much of which the government is not entitled to have, all at the expense of their speedy trial rights.

In *United States v. Hunter*, 13 F.Supp.2d 574, 584 (D.Vermont), the court held as follows:

To withstand an overbreadth challenge, the search warrant itself, or materials incorporated by reference, must have specified the purpose for which the computers were seized and delineated the limits of their subsequent search. Section IV was insufficiently particularized, and all computer equipment and disks seized under that paragraph were taken in violation of the Fourth Amendment's particularity requirement.

Similarly, in the context of a subpoena, Judge Mukasey noted that "the government acknowledged that a 'key search' of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation.'" The court quashed a subpoena that called for specified computer hard drives and floppy disks "that contain some data concededly irrelevant to the grand jury inquiry. *IN re Grand Jury Subpoena Duces Tecum*, 846 F.Supp. 11, 12-13 (S.D.N.Y. 1994).

Page 3
March 17, 2006

The Court should therefore order the government to provide a list of search terms, subject to challenge and a final ruling by the Court. After the appropriate searches are run, the material should be segregated and the rest returned to the defendants or otherwise made unavailable to the government. This will at least ameliorate the tremendous burden on both parties of having to litigate privilege in a case involving a mind-boggling amount of computer information.

Respectfully submitted,

HOFFMAN & POLLOK

By; _____
Susan C. Wolfe

Cc: Marc Litt, AUSA